EXHIBIT B

2023 WL 5029899
Only the Westlaw citation is currently available.
United States District Court, N.D. California.

Chasom BROWN, et al., Plaintiffs,
v.
GOOGLE LLC, Defendant.

Case No.: 4:20-cv-3664-YGR
|
Signed August 7, 2023

Synopsis

Background: Account holders of internet-search company brought class action, alleging that company unlawfully collected data from account holders while they used company's or third-party browsers in private or incognito mode, and bringing claims under the federal Wiretap Act, the California Invasion of Privacy Act (CIPA), California's Comprehensive Data Access and Fraud Act (CDAFA), and California's Unfair Competition Law (UCL), as well as claims for invasion of privacy under the California Constitution, intrusion upon seclusion, and breach of contract. Company moved for summary judgment, account holders moved to strike parts of company's reply brief, and the parties brought various motions to seal.

Holdings: The District Court, Yvonne Gonzalez Rogers, J., held that:

account holders alleged a sufficiently concrete harm to support Article III standing;

account holders had standing to seek a quasi-contractual remedy based on unjust enrichment and to seek injunctive relief;

genuine issues of material fact precluded summary judgment for company based on its defense asserting that account holders gave consent to challenged practices;

genuine issues of material fact over the terms of contract between account holders and company precluded summary judgment for company on breach-of-contract claim;

contract between account holders and company was not invalid for lack of consideration;

genuine issues of material fact precluded summary judgment for company on Wiretap Act, CIPA, and CDAFA claims;

account holders had a reasonable expectation of privacy in data at issue, as required to state claims for invasion of privacy and intrusion upon seclusion;

genuine issues of material fact over the offensiveness of the challenged practices precluded summary judgment for company on account holders' claims for invasion of privacy and intrusion upon seclusion;

account holders alleged a sufficient economic injury to support their UCL claim; and

account holders lacked an adequate remedy at law and thus were not barred from bringing their UCL claim.

Company's motion for summary judgment denied; account holders' motion to strike denied as moot; motions to seal denied as to information relied on in order but otherwise conditionally granted.

Procedural Posture(s): Motion for Summary Judgment; Motion to Strike; Motion to Seal Records.

Attorneys and Law Firms

John A. Yanchunis, Jean Sutton Martin, Olusegun Amen, Ra, Ryan McGee, Morgan & Morgan Complex Litigation Group, Tampa, FL, Alexander Patrick Frawley, Pro Hac Vice, Ryan Sila, Pro Hac Vice, Steven M. Shepard, Pro Hac Vice, William Christopher Carmody, Amy B. Gregory, Pro Hac Vice, Shawn Jonathan Rabin, Susman Godfrey LLP, New York, NY, Samuel Issacharoff, New York, NY, Alexander Justin Konik, Beko Osiris Ra Reblitz-Richardson, Erika Britt Nyborg-Burch, Sean Phillips Rodriguez, Mark C. Mao, Boies Schiller Flexner LLP, San Francisco, CA, Michael Francis Ram, Morgan & Morgan Complex Litigation Group, San Francisco, CA, Alison Lynn Anderson, Logan Wright, Boies Schiller Flexner LLP, Los Angeles, CA, Amanda K. Bonn, Susman Godfrey L.L.P., Los Angeles, CA, David Boies, Boies Schiller and Flexner, Armonk, NY, James W. Lee, Rossana Baeza, Boies Schiller Flexner, Miami, FL, Jenna Golda Farleigh, Susman Godfrey L.L.P., Seattle, WA, for Plaintiff Chasom Brown.

John A. Yanchunis, Jean Sutton Martin, Olusegun Amen, Ra, Ryan McGee, Morgan & Morgan Complex Litigation Group, Tampa, FL, Alexander Patrick Frawley, Pro Hac Vice, Ryan Sila, Pro Hac Vice, Steven M. Shepard, Pro Hac Vice, William Christopher Carmody, Amy B. Gregory, Shawn Jonathan Rabin, Susman Godfrey LLP, New York, NY, Samuel Issacharoff, New York, NY, Alexander Justin Konik, Beko Osiris Ra Reblitz-Richardson, Sean Phillips Rodriguez, Mark C. Mao, Boies Schiller Flexner LLP, San Francisco, CA, Amanda K. Bonn, Susman Godfrey L.L.P., Los Angeles, CA, David Boies, Boies Schiller and Flexner, Armonk, NY, James W. Lee, Rossana Baeza, Boies Schiller Flexner, Miami, FL, Jenna Golda Farleigh, Susman Godfrey L.L.P., Seattle, WA, for Plaintiff Maria Nguyen.

John A. Yanchunis, Jean Sutton Martin, Olusegun Amen, Ra, Ryan McGee, Morgan & Morgan Complex Litigation Group, Tampa, FL, Alexander Patrick Frawley, Pro Hac Vice, Ryan Sila, Pro Hac Vice, Steven M. Shepard, Pro Hac Vice, William Christopher Carmody, Amy B. Gregory, Shawn Jonathan Rabin, Susman Godfrey LLP, New York, NY, Samuel Issacharoff, New York, NY, Alexander Justin Konik, Beko Osiris Ra Reblitz-Richardson, Erika Britt Nyborg-Burch, Sean Phillips Rodriguez, Mark C. Mao, Boies Schiller Flexner LLP, San Francisco, CA, Alison Lynn Anderson, Logan Wright, Boies Schiller Flexner LLP, Los Angeles, CA, Amanda K. Bonn, Susman Godfrey L.L.P., Los Angeles, CA, David Boies, Boies Schiller and Flexner, Armonk, NY, James W. Lee, Rossana Baeza, Boies Schiller Flexner, Miami, FL, Jenna Golda Farleigh, Susman Godfrey L.L.P., Seattle, WA, for Plaintiff William Byatt.

Aarti G. Reddy, Cooley LLP, San Francisco, CA, Jonathan Sze Ming Tse, Quinn Emanuel Urquhart and Sullivan LLP, San Francisco, CA, Alyssa G. Olson, Stephen Andrew Broome, Viola Trebicka, Crystal Nix-Hines, Marie M. Hayrapetian, Quinn Emanuel Urquhart Sullivan LLP, Los Angeles, CA, Andrew H. Schapiro, Pro Hac Vice, Joseph H. Margolies, Pro Hac Vice, Teuta Fani, Quinn Emanuel Urquhart and Sullivan, LLP, Chicago, IL, Brett Watkins, Pro Hac Vice, Quinn Emanuel Urquhart and Sullivan LLP, Houston, TX, Carl Spilly, Pro Hac Vice, Washington, DC, Xi Gao, Quinn Emanuel Urquhart Sullivan, LLP, Washington, DC, Diane M. Doolittle, Sara E. Jenkins, Quinn Emanuel Urquhart & Sullivan, LLP, Redwood Shores, CA, Donald Seth Fortenbery, New York, NY, Jomaire Alicia Crawford, Pro Hac Vice, Josef Teboho Ansorge, Pro Hac Vice, Quinn Emanuel Urquhart and Sullivan, LLP, New York, NY, for Defendant.

ORDER DENYING GOOGLE'S MOTION FOR SUMMARY JUDGMENT;

DENYING PLAINTIFFS' MOTION TO STRIKE;

ADDRESSING PARTIES' MOTIONS TO SEAL

Re: Dkt. Nos. 907, 908, 924, 933, 936, 937, 939, 942, 945

Yvonne Gonzalez Rogers, United States District Court Judge

***1** Plaintiffs Chasom Brown, William Byatt, Jeremy Davis, Christopher Castillo, and Monique Trujillo bring this class action based on Google's "surreptitious interception and collection of personal and sensitive user data while users are in 'private browsing mode.' " (Dkt. No. 886, Fourth Amended Complaint, "4AC" ¶ 1.) The 4AC contains seven counts: (1) violation of the Federal Wiretap Act, 18 U.S.C. § 2510, *et seq.*; (2) violation of the California Invasion of Privacy Act ("CIPA"), California Penal Code §§ 631 and 632; (3) violation of the Comprehensive Data Access and Fraud Act ("CDAFA"), Cal. Pen. Code § 502, *et seq.*; (4) invasion of privacy; (5) intrusion upon seclusion; (6) breach of contract; and (7) violation of California's Unfair Competition Law ("UCL"), Cal. Bus. & Prof. Code § 17200, *et seq.* Google brings a Motion for Summary Judgment on all counts and parties both submitted several administrative motions to seal. (Dkt. Nos. 907, 908, 924, 933, 936, 937, 939, 942, 945.) Having carefully considered the parties' briefing, the admissible evidence, the record in this case, and upon further consideration after the May 12, 2023, oral argument, the Court **DENIES** Google's motion for summary judgment. [1] Google's motion hinges on the idea that plaintiffs consented to Google collecting their data while they were browsing in private mode. Because Google never explicitly told users that it does so, the Court cannot find as a matter of law that users explicitly consented to the at-issue data collection.

I. BACKGROUND

The parties have hotly disputed this action from the start. For the sake of brevity, the Court gives only the background relevant to the resolution of Google's motion for summary judgment.

A. FACTUAL BACKGROUND

1. Data Collection

Plaintiffs are Google account holders who used two types of "private browsing modes": Incognito mode, which is found on Google's Chrome browser, and the private browsing mode of other browsers.[2] (4AC ¶ 192.) Since June 1, 2016, Google represented to plaintiffs it would not collect their information while they browsed privately. (*Id.* ¶ 2.) It did so anyway, collecting, aggregating, and selling plaintiffs' private browsing data without their consent. (*Id.* ¶ 4.)

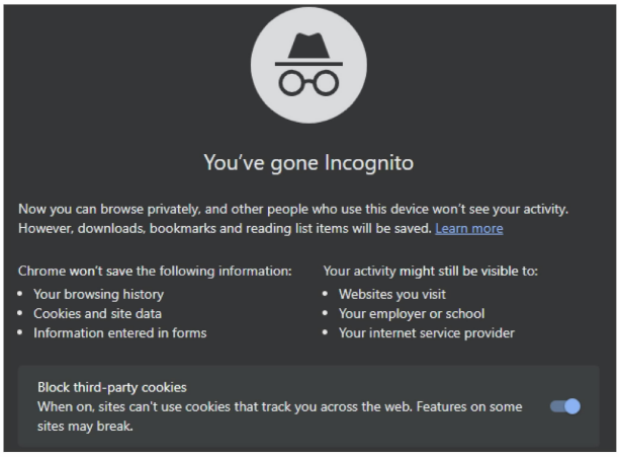
***2** Whenever a user visits a website that is running Google Analytics, Ad Manager, or some similar Google service, Google's software directs the user's browser to send a separate communication to Google. (*Id.* ¶ 63.) This happens even when users are in private browsing mode, unbeknownst to website developers or the users themselves. (*Id.* ¶ 66.) The operation is not in dispute. (PAF 10.)[3] When a user visits a website, the user's browser sends a "GET" request to the website to retrieve it. (*Id.*) This GET request contains the following information: the Request URL, or the URL of the specific webpage the user is trying to access; the user's IP address; the User-agent, which identifies the user's device platform and browser; user's geolocation, if available; the Referer, which is the URL of the page on which the user clicked a link to access a new page; event data, which describes how users interact with a website, for example, whether they saw an ad or played a video; and the actual search queries on the site. (*Id.*) At the same time, the user's browser reads Google's code, which is embedded on the website. (*Id.*) Google's code instructs the user's browser to send a second and concurrent transmission directly to Google. (*Id.*) This second transmission tells Google exactly what a user's browser communicated to the website. (*Id.*)

Google's services are ubiquitous on the internet: over 70 percenta of websites use Google Analytics and Ad Manager. (4AC ¶¶ 67 and 78.) To use these services, Google requires website developers to embed Google's code onto their websites and agree to its Privacy Policy. (PAF 6.) Google does not tell website developers that it tracks their visitors even when they are in private browsing mode. (*Id.*)

According to plaintiffs, Google then takes users' private browsing history and associates it with their preexisting user profiles. (PAF 47; Response to SUF 65.) Doing so allows Google to offer better, more targeted, advertisements to users. (Response to SUF 63; 4AC ¶ 84.) This is at the core of Google's business: the bulk of Google's hundreds of billions of dollars in revenue come from selling targeted advertisements to other companies. (4AC ¶ 89.) By selling users' information, Google prevents users from monetizing their own data. (4AC ¶ 138; PAF 27–28.) The value of this data can be quantified; for example, Google itself has piloted a program to pay users $3.00 per week to track them. (PAF 28.)

2.Google's Representations About Private Browsing Modes

The parties do not dispute that Google's General Terms of Service and its Chrome Privacy Notice are the basis of the contract between Google and its accountholders.[4] (SUF 15.) Further, they agree that Google's Privacy Policy was incorporated up until March 2020. That said, plaintiffs assert that three other writings are incorporated into this contract: One, Google's Privacy Policy (post March 2020), which is hyperlinked in the latest version of its General Terms of Service. (Dkt. No. 908-14, Ex. 112, 12/15/22 Google Privacy Policy.) Google's Privacy Policy tells users it is "meant to help you understand what information we collect, why we collect it, and how you can update, manage, export, and delete your information." (*Id.*) Two, the Search & Browse Privately Help page, which is hyperlinked in that Privacy Policy. (Dkt. No. 908-8, Ex. 92, 3/5/22 Search & Browse Privately Help page.) This page tells users "you're in control of what you information you share with Google when you search." Three, the Incognito Splash Screen, which is the first thing users see when they access Incognito mode. (Dkt. No. 908-4, Ex. 74, Incognito Splash Screen.) The Splash Screen tells users:



B. PROCEDURAL BACKGROUND

Given the parties' briefing, the Court notes the following procedural background:

On June 2, 2020, plaintiffs filed this suit. Initially, plaintiffs brought five counts: (1) unauthorized interception under the Wiretap Act; (2) violation of CIPA; (3) violation of CDAFA; (4) invasion of privacy; and (5) intrusion upon seclusion. Google then filed its first motion to dismiss all five claims. Then-District Court Judge Koh denied the motion to dismiss. *Brown v. Google*, 525 F.Supp.3d 1049 (N.D. Cal. 2021) (*Brown I*). Plaintiffs then added two more counts: (6) breach of contract and (7) violation of the UCL. Again, Judge Koh denied Google's motion to dismiss those two counts. *Brown v. Google*, 20-cv-3664-LHK, 2021 WL 6064009 (N.D. Cal. Dec. 22, 2021) (*Brown II*).

***3** Relevant here, individual plaintiffs brought this suit on behalf of two classes: Class 1, for Incognito users, and Class 2, for users of other private browsing modes. Plaintiffs asked this Court to certify both classes under Federal Rules of Civil Procedure 23(b)(2) and (3). The Court granted this request only in part. (Dkt. No. 803.) Although it found that plaintiffs could seek injunctive relief on a classwide basis, it denied plaintiffs' request for a damages class because an individual issue—whether plaintiffs impliedly consented to Google's data collection here—predominated. (*Id.*) Thereafter, Google brought this summary judgment motion against all of plaintiffs' claims.

II. LEGAL FRAMEWORK

A party may move for summary judgment on a "claim or defense." Fed. R. of Civ. P. 56(c). As a general matter, where the party moving for summary judgment would bear the burden of proof at trial, it bears the initial burden of proof at summary judgment as to each material fact and must show that no reasonable jury could find other than for the moving party. *See S. California Gas Co. v. City of Santa Ana*, 336 F.3d 885, 888 (9th Cir. 2003) (internal citation omitted). Summary judgment is appropriate only when "there is no genuine dispute as to any material fact and the movant is entitled to judgment as a matter of law." Fed. R. of Civ. P. 56(a). To determine if this is so, the court must view all evidence in the light most favorable to the nonmoving party and draw all justified inferences on its behalf. *Anderson v. Liberty Lobby, Inc.*, 477 U.S. 242, 248, 106 S.Ct. 2505, 91 L.Ed.2d 202 (1986).

III. ANALYSIS

A. MOTION AS TO ALL COUNTS

Google seeks judgment on all seven counts on two overarching grounds. First, Google argues that plaintiffs lack standing to bring any of their claims. Second, Google contends that, because plaintiffs expressly consented to Google tracking them in private browsing mode, all of plaintiffs' claims fail. The Court examines each.

1. Standing

"To have Article III standing to sue in federal court, plaintiffs must demonstrate, among other things, that they have suffered a concrete harm." *TransUnion LLC v. Ramirez*, —— U.S. ——, 141 S.Ct. 2190, 2200, 210 L.Ed.2d 568 (2021). To determine what harms are sufficiently concrete for purposes of Article III, the Supreme Court has explained that "history and tradition offer a meaningful guide." *Id.* at 2204 (cleaned up). Certain harms "readily qualify as concrete injuries under Art. III. The most obvious are traditional tangible harms, such as physical harms and monetary harms." *Id.* Intangible harms, such as disclosure of private information or intrusion upon seclusion, have also been traditionally recognized. *Id.*; *see also Eichenberger v. ESPN*, 876 F.3d 979, 983 (9th Cir. 2017) (noting that "[v]iolations of the right to privacy have long been actionable at common law").

"As the party invoking federal jurisdiction, the plaintiffs bear the burden of demonstrating that they have standing." *Id.* 2207. That burden changes as litigation develops. "In response to a summary judgment motion," plaintiffs must demonstrate standing for each claim that they press and for each form of relief that they seek (for example, injunctive relief and damages)." *Id.* at 2208. That said, "the threshold question of whether plaintiff has standing (and the court has jurisdiction) is distinct from the merits of [their] claim." *Maya v. Centex Corp.*, 658 F.3d 1060, 1068 (9th Cir. 2011).

For each of the seven counts,[5] plaintiffs assert standing for two types of harm: breach of contract and invasion of privacy. They also seek two types of remedy: unjust enrichment and injunctive relief. The Court analyzes each.

a. Standing as it Relates to the Nature of Harm

i. Breach of Contract

***4** Plaintiffs allege that they suffered harm under a breach of contract theory for Counts Six—breach of contract—and Seven—violation of California's UCL. (4AC ¶ 272.) Plaintiffs proffer evidence that Google promised plaintiffs it would not collect their data while they were in private browsing mode and that it did so anyway. Google argues this is not enough—plaintiffs must show an additional concrete harm. According to Google, even assuming plaintiffs' position, users will not have suffered a concrete harm. The Court disagrees.

The "longstanding common law rule in most states," including California, is that "the failure to perform a duty required by contract is a legal wrong, independently of actual damage sustained by the party to whom performance is due." *In re Google Referrer Header Privacy Litig.*, 465 F. Supp. 3d 999, 1010 (N.D. Cal. 2020) (citing *Kenyon v. W. Union Tel. Co.*, 100 Cal. 454, 458, 35 P. 75 (1893) and 22 Am. Jur. 2d Damages § 17). In a suit for a violation of a private right—including "contract rights"—"courts historically presumed that the plaintiff suffered a *de facto* injury merely from having [their] personal, legal rights invaded." *Spokeo, Inc. v. Robins*, 578 U.S. 330, 344, 136 S.Ct. 1540, 194 L.Ed.2d 635 (2016) (Thomas, J. concurring). That is why "a breach of contract claim accrues at the moment of breach and the injury, for standing purposes, is the breach itself." *In re Google Referrer*, 465 F. Supp. 3d at 1011 (citing *Alston v. Flagstar Bank, FSB*, 609 Fed. App'x 2, 3 (D.C. Cir. 2015)).

Nothing in *TransUnion* requires otherwise. As the Supreme Court held, the answer to what constitutes a concrete harm is rooted in historical practice. *TransUnion*, 141 S.Ct. at 2204. Plaintiffs can point to a "close historical or common-law analogue" to bring suit in federal court. *Id.* The instant action does not "merely seek[ ] to ensure a defendant's compliance with regulatory law" or to remedy a "bare procedural violation." *Id.* at 2206 (citing *Spokeo*, 578 U.S. at 345, 136 S.Ct. 1540 (Thomas, J. concurring)). Rather, plaintiffs allege a substantive breach of a private contract. *Cf. Spokeo*, 578 U.S. at 341, 136 S.Ct. 1540. That is sufficient for standing. As the Ninth Circuit recognized in finding standing for the same causes of action, "in an era where millions of Americans conduct their affairs increasingly through electronic devices, the assertion that federal courts are powerless to provide a remedy when an internet company surreptitiously collects private data is untenable." *In re Facebook, Inc. Internet Tracking Litig.*, 956 F.3d 589, 599 (9th Cir. 2020) (citing *In re Google Inc. Cookie Placement Consumer Privacy Litig.*, 934 F.3d 316, 325 (3rd Cir. 2019) (cleaned up)).

It is true, as Google notes, that some courts in this district have found that a breach of contract alone does not confer Article III standing. *In re Google Referrer*, 465 F.Supp.3d at 1011 (collecting cases). Those cases are inapplicable because in each of them plaintiffs sought only nominal damages. *See, e.g. Svenson v. Google Inc.*, No. 13-cv-4080, 2016 WL 8943301 (N.D. Cal. Dec. 21, 2016). Here, plaintiffs are requesting actual damages and injunctive relief.

The Court finds that plaintiffs have standing to bring their breach of contract and UCL claims. Google's summary judgment motion on this point is **DENIED.**

ii. Invasion of Privacy

With respect to the balance of the 4AC,[6] plaintiffs root standing in a harm to privacy. Google responds that plaintiffs' harm is not concrete enough to confer standing because it does not associate private browsing data with users' profiles.

***5** The Supreme Court has noted that certain torts, like the disclosure of private information and intrusion upon seclusion claims brought here, result in "intangible" but concrete harms. *TransUnion*, 141 S.Ct. at 2204. Where, as here, plaintiffs allege privacy harms in the context of both statutory and common law violations, courts are "guided in determining concreteness by both history and the judgment of Congress, or the legislature that enacted the statute." *Campbell v. Facebook, Inc.*, 951 F.3d 1106, 1116 (9th Cir. 2020) (cleaned up). Where a statute codifies procedural rights, the Supreme Court has held that their violation "would not invariably injure a concrete interest." *Eichenberger*, 876 F.3d at 982 (citing *Spokeo*, 136 S.Ct. at 1549). In contrast, the violation of a statute that protects a "*substantive* right to privacy" does result in a concrete harm. *Id.* "Tellingly, privacy torts do not always require additional consequences to be actionable." *Eichenberger*, 876 F.3d at 983 (citing Restatement (Second) of Torts § 652B cmt. b. (Am. Law Inst. 1977)). The intrusion into privacy itself is what makes a defendant liable. *Id.*

The Ninth Circuit has found that each of the statutory claims brought here codify substantive rights to privacy. *See In re Facebook Tracking*, 956 F.3d at 598 (so holding for violations of the Wiretap Act, CIPA, CDAFA); *Campbell*, 951 F.3d at 1117–18 (so holding for UCL claims that were based

on Wiretap Act and CIPA violations). Because plaintiffs' claims also "arise under the core provisions of those statutes," this Court finds that plaintiffs have Article III standing. *See Campbell*, 951 F.3d at 1118; *see also Phillips v. United States Customs and Border Prot.*, 74 F.4th 986, —— (9th Cir. 2023) (noting that *Campbell* is "consistent with many other cases in which we held that the plaintiffs had standing to challenge the retention of illegally obtained records because the retention amounted to an invasion of their privacy interests"). [7]

Google's argument that privacy harms are never concrete where only anonymized data is collected does not persuade given the evidence presented here. *See Campbell*, 951 F.3d at 1112. In *Campbell*, Facebook also argued that the plaintiffs lacked standing because the data at issue was "***anonymized*** and ***aggregated***." *Facebook's Supplemental Br. Re: Spokeo, Inc. v. Robins*, No. 17-16873, 2019 WL 2396054, at *1 (9th Cir. 2019). The Ninth Circuit disagreed. The court held that the only reason Facebook could access and use that data was because the users did not consent to the "collection and storage of information from private messages" from those users. *Id.* In short, because plaintiffs alleged that the defendant had collected their data "without consent," Facebook had violated the "concrete privacy interests" that statutes like the Wiretap Act and CIPA protect, "regardless of how the collected data was later used." *Id.* So too here. Plaintiffs have set forth specific facts demonstrating that the reason Google has access to their anonymous, aggregated data is through the collection and storage of information from users' private browsing history without consent. [8] That is enough, under *Campbell*, to confer standing given the sensitivity of the evidence at issue. [9] That Google has a different view on the evidence does not mean that plaintiffs' lack standing.

***6** Google's other cited authorities do not compel a different result. [10] Rather, those cases confirm that the standing analysis is contextual. *See, e.g., Facebook Tracking*, 956 F.3d at 589–99 (finding standing not just because Facebook correlated data collected with users' profiles but also because Facebook had promised not to collect users' data after they logged out but did so anyway); *I.C. v. Zynga, Inc.*, 600 F.Supp.3d 1034, 1049 (N.D. Cal. 2022) (finding a lack of standing where data at issue was not as sensitive as shown here, such as basic contact information, including one's email address, phone number, or Facebook or Zynga username, is private information).

What is more, plaintiffs set forth evidence that Google does store their data with unique identifiers. (PAF 25.) [11] For example, plaintiffs have evidence that Google stores users' regular and private browsing data in the same logs; it uses those mixed logs to send users personalized ads; and, even if the individual data points gathered are anonymous by themselves, when aggregated, Google can use them to "uniquely identify a user with a high probability of success." (Dkt. No. 907-7, Ex. 77 ¶ 105.) This supports plaintiffs' showing that they suffered concrete harm.

For those reasons, the Court finds that plaintiffs have standing for counts One through Five. Google's motion for summary judgment on this point is **DENIED.**

b. Standing as it Relates to the Nature of the Remedy

i. Quasi-Contract: Unjust Enrichment

For three of their counts (breach of contract and violation of both the CDAFA and UCL), plaintiffs seek a quasi-contractual remedy of unjust enrichment. (4AC ¶¶ 233, 274, 284.) Google argues that, because unjust enrichment is not a remedy available to Rule 23(b)(2) classes, plaintiffs lack standing. Plaintiffs disagree and note that all class members also seek individual damages. In addition, plaintiffs have evidence that there is a market for this data—Google itself piloted a program to pay users $3.00 a month to collect their browsing data. (PAF28).

***7** The Court concurs. Plaintiffs have sufficiently shown that Google profited from their personal browsing histories and thus a remedy based upon unjust enrichment may lie. *See Facebook Tracking*, 956 F.3d at 600 ("Because California law recognizes that individuals maintain an entitlement to unjustly earned profits, to establish standing, Plaintiffs must allege that they retain a stake in the profits garnered from their personal browsing histories.").

For those reasons, Google's motion for summary judgment as to plaintiffs' lack of standing to bring their unjust enrichment remedy is **DENIED.**

ii. Injunctive Relief

To establish standing for prospective injunctive relief, a plaintiff must demonstrate "continuing, present adverse effects." *City of Los Angeles v. Lyons*, 461 U.S. 95, 102, 103 S.Ct. 1660, 75 L.Ed.2d 675 (1983) (cleaned up). Plaintiffs seek the following injunctive relief for all seven counts: a permanent restraint on Google "intercepting, tracking, or collecting communications after class members used a browser while in 'private browsing mode,' or otherwise violating its policies with users." (4AC at 72.) Google argues that plaintiffs cannot show that the risk of harm is sufficiently imminent and substantial to confer standing for injunctive relief. The Court disagrees. Google's conduct has not stopped. Plaintiffs have demonstrated that absent an injunction, Google will continue to collect users' private browsing data for its own use without users' express consent.

Google's motion for summary judgment as to plaintiffs' lack of standing to seek an injunctive remedy is **DENIED.**

2. Express Consent [12]

Next, Google argues that the Court should grant summary judgment as to all of plaintiffs' claims because users expressly consented to Google collecting their data while they were in private browsing mode. [13] Plaintiffs disagree.

As this Court has previously noted, consent "can be explicit or implied, but any consent must be actual." *In re Google RTB Consumer Privacy Litig.*, 606 F.Supp.3d 935, 949 (N.D. Cal. 2022) (cleaned up). For consent to be actual, the disclosures must "explicitly notify" users of the practice at issue. *Id.* (cleaned up). In other words, consent is only effective if the person alleging harm consented "to the particular conduct, or to substantially the same conduct" and if the alleged tortfeasor did not exceed the scope of that consent. Restatement (Second) of Torts § 892A (1979) §§ 2(b), 4.

Relying on *Calhoun* [14], Google argues that its Privacy Policy unambiguously [15] discloses the data collection challenged here because it is mode-agnostic, that is, Google collects the same data whether users are in regular or private browsing mode. Said differently, Google argues summary judgment is appropriate because it disclosed that it collects users' data in general, even if it did not disclose that it collects users' private browsing data in particular. Plaintiffs, by contrast, claim that because Google portrayed Incognito mode, for example, as affording more privacy than regular browsing mode, a reasonable user could have concluded that Google's data collection was not mode-agnostic. [16]

***8** The analysis starts with the Privacy Policy [17] wherein Google advises at the outset and in bold, larger print:

> **When you use our services, you're trusting us with your information. We understand this is a big responsibility and work hard to protect your information and put you in control.**

(12/15/22 Google Privacy Policy.) Immediately after, Google advises:

> This Privacy Policy is meant to help you understand what information we collect, why we collect it, and how you can update manage, export, and delete your information.
>
> * * *
>
> We build a range of services that help millions of people daily to explore and interact with the world in new ways. Our services include:
>
> • Google apps, sites, and devices, like Search, YouTube, and Google Home
>
> • Platforms like the Chrome browser and Android operating system
>
> • Products that are integrated into third-party apps and sites, like ads and embedded Google Maps

(*Id.*) Notably, Incognito mode is not mentioned in this list of services. (*Id.*) Rather, Google shifts and in the next paragraph advises users: "You can use our services in a variety of ways to manage your privacy ... You can also choose to browse the web in a private mode, like Chrome Incognito mode. And across our services, you can adjust your privacy settings to control what we collect and how your information is used." [18] (*Id.*) That is the only mention made of the privacy mode. The Privacy Policy is silent as to any data collection specific to private browsing mode.

The Court rejects Google's argument that the Privacy Policy unambiguously discloses the at-issue data collection. The

silence noted above combined with Google's surrounding statements regarding what it means to "browse privately," means that a material dispute of fact remains regarding the scope of users' consent. For instance, the way Google presents Incognito mode could be read to contradict its suggested interpretation of the Privacy Policy. When users first open Chrome, they are greeted by a bright, white screen and the colorful Google logo. When users navigate to Incognito mode, the screen goes from white to black, all text is rendered in gray, and users are met with a "spy guy icon." (PAF 9.) They are told they have now "gone Incognito," which, Google explains on the next line, means that they can "browse privately, and other people who use this device won't see your activity." (PAF 30.) Plaintiffs have evidence to show that, internally, Google understood that the "framing of the feature as 'Incognito' (or, for other browsers, 'Private')" made users "overestimate privacy mode protections," including that Incognito "hides browsing activity from Google." (Dkt. No. 924-36, Ex. 80; Dkt. No. 924-48, Ex. 44.)

***9** Google's arguments otherwise do not change the result. Its reliance on this Court's finding in *Calhoun* is misplaced. That case did not involve Incognito mode. *See Calhoun*, ——F.Supp.3d at ——, 2022 WL 18107184, at *10. The reasoning therefore does not extend here.

Next, Google argues that to obtain consent effectively, companies should not have to enumerate every mode, setting, or circumstance impacting—or *not* impacting—that data collection. *See Smith v. Facebook, Inc.*, 745 Fed. App'x 8, 9 (9th Cir. 2018) (holding that Facebook's tracking of publicly available health data fell within the scope of users' general consent to its data tracking and collection practices). It is true that such enumeration is not always necessary. The fundamental issue, however, returns to actual consent. Google chose both to use a general disclosure and yet promote the privacy afforded by Incognito over regular mode. Having made that distinction, Google itself created a situation where there is a dispute as to whether users' consent of Google's data collection generally is "substantially the same" as their consent to the collection of their private browsing data in particular. *See* Restatement (Second) of Torts § 892A (1979) §§ 2(b), 4.

For those reasons, the Court **DENIES** Google's motion for summary judgment on the grounds of express consent.

B. MOTION AS TO INDIVIDUAL COUNTS

Next, Google argues that plaintiffs' seven claims fail for individual reasons. The Court analyzes each.

1. Breach of Contract

Google seeks judgment on plaintiffs' breach of contract claim on two grounds, one relative to which writings form the contract and the second on the alleged promises made therein.

a. Incorporation

As set forth above, the parties agree that their contract includes Google's General Terms of Service, the Chrome Privacy Notice, and Google's Privacy Policy (but only through March 2020).[19] They dispute whether three other writings are incorporated into the contract: the post-March-2020 Privacy Policy, the Search & Browse Privately Help page, and the Incognito Splash Screen.

Under California law, "[a] contract may validly include the provisions of a document not physically a part of the basic contract." *Shaw v. Regents of University of California*, 58 Cal.App.4th 44, 54, 67 Cal.Rptr.2d 850 (1997) (internal quotation omitted). "For the terms of another document to be incorporated into the document executed by the parties the reference must be clear and unequivocal, the reference must be called to the attention of the other party and [they] must consent thereto, and the terms of the incorporated document must be known or easily available to the contracting parties." *Id.* "The contract need not recite that it 'incorporates' another document, so long as it guides the reader to the incorporated document." *Id.* (cleaned up). Whether a writing is incorporated is a context-specific inquiry. *Id.*

10** ***Post-March-2020 Privacy Policy. Google argues that its Privacy Policy has not been incorporated into the parties' underlying contract since March 2020.[20] By way of background, before March 2020, Google's Terms of Service explicitly stated:

> Google's privacy policies explain how we treat your personal data and protect your personal privacy when you use our Services. By using our Services, you agree that Google can use such

> data in accordance with our privacy policies.

(Dkt. No. 908-17, Ex. 136.) Then, on March 31, 2020, Google changed its Terms of Service to read:

> [W]e also publish a Privacy Policy. *Although it's not part of these terms*, we encourage you to read it to better understand how you can update, manage, export, and delete your information.

(Dkt. No. 908-17, Ex. 137 (emphasis supplied).) Given this express disavowal, Google argues that the post-March-2020 Privacy Policy is no longer incorporated.

The evidence presented, however, is not entirely as unequivocal as Google suggests. First, and notably, Google changed its Terms of Service again on January 5, 2022, to state:

> In addition to these terms, we also publish a Privacy Policy (hyperlink). *We encourage you to read it to better understand how you can update, manage, export and delete your information* .... You also agree that our Privacy Policy (hyperlink) applies to your use of services.

(Emphasis supplied.) (Dkt. No. 908-17, Ex. 138.) In the post-January-2022 Terms of Service, Google suggests that the Privacy Policy does apply, raising a triable issue as to whether the Privacy Policy was incorporated in the interim. Second, Google ignores the language of the Chrome Privacy Notice.[21] The post-March-2020 Chrome Privacy Notice states, repeatedly, that "any personal information that is provided to Google or stored in your Google Account will be used and protected in accordance with the Google Privacy Policy (hyperlink), as changed from time to time." (Dkt. No. 908-16, Ex. 130, 5/20/20 Chrome Privacy Notice.) Again, the Notice indicates that Google's Privacy Policy could be incorporated.

Accordingly, there is at least a triable issue as to whether the Privacy Policy in effect after March 2020 was incorporated.

Search & Browse Privately Help Page. Next, plaintiffs assert that the Search & Browse Privately page is incorporated because the Privacy Policy specifically tells users to "search and browse privately (hyperlink)," language that hyperlinks to the Search & Browse Privately page. (12/15/22 Google Privacy Policy.) The Court agrees. Because the Privacy Policy "guides" users to this page, users could have reasonably concluded that its terms applied.

***11** Google's reliance on *Rodriguez*[22] does not compel a different result. There, Google argued that the "WAA Help Page" was not incorporated into its privacy policy. *Id.* The court agreed and found that the "mere fact of a hyperlink" was not enough for incorporation, *id.* at *4, "[a]s opposed to a hyperlink embedded within language signifying the linked material—*e.g.*, learn more by visiting the WAA Help Page," *id.* at n.4. Here, the hyperlink *is* embedded within language that references the title of the linked page: The Privacy Policy tells users to "search and browse privately (hyperlink)."

Incognito Splash Screen. Finally, Google argues that the Incognito Splash Screen is not incorporated. Plaintiffs disagree. Both the Privacy Policy[23] and Chrome Privacy Notice invite users to use Incognito mode. It is impossible to use Incognito mode without seeing the Splash Screen. For that reason, plaintiffs argue, the Splash Screen is incorporated. Again, the Court agrees that there is at least a triable issue. Because the Chrome Privacy Notice and Privacy Policy necessarily guide users to the Splash Screen, a reasonable user could conclude it is part of the parties' contract.

Plaintiffs have therefore identified sufficient evidence raising a triable issue of fact that all three writings were incorporated. Summary judgment on this ground is **DENIED.**

b. Enforceable Promises

Next, the parties dispute whether any of the writings articulate a contractual promise not to collect, track, and use plaintiffs' private browsing activity. In support, plaintiffs point to the following statements:

- **Chrome Privacy Notice:** Google promises that it does not collect or use private browsing communications by explaining: "You can limit the information Chrome stores on your system by using Incognito mode," and that within Incognito mode "Chrome won't store certain information such as: Basic browsing history information like URLs, cached page text, or IP addresses of pages linked from the website you visit [and] Snapshots of pages that you visit." (5/20/20 Chrome Privacy Notice.)

- **Privacy Policy:** Since May 2018, the Privacy Policy has represented: "[A]cross our services, you can adjust our privacy settings to control what we collect and how your information is used"; "you can use our services in a variety of ways to manage your privacy. For example ... [y]ou can [ ] choose to browse the web privately using Chrome in Incognito mode." Since February 2022, the Privacy Policy has also stated: "You can also choose to browse the web in a private mode, like Chrome incognito mode." (12/15/22 Google Privacy Policy.)

- **Incognito Splash Screen:** The Incognito Splash Screen's statement that: "Now you can browse privately, and other people who use this device won't see your activity." (Incognito Splash Screen.) "Chrome won't save ... [y]our browsing history [or] cookies and site data." (*Id.*) The omission of Google from the list of entities "[y]our activity might still be visible to." (*Id.*)

- **Search & Browse Privately Page:** This page starts by stating: "You're in control of what information you share with Google when you search. To browse the web privately, you can use private browsing." (3/5/22 Search & Browse Privately Help page.) This page explains further that "[i]f you want to search the web without saving your search activity to your account, you can use private browsing mode in a browser (like Chrome or Safari)" (*Id.*) [24]

***12** Taken as a whole, a triable issue exists as to whether these writings created an enforceable promise that Google would not collect users' data while they browsed privately. [25] For example, in its Privacy Policy, Google tells users that they "control" what Google collects and how their "information is used." One way to do that, Google tells users, is by using a private browsing mode like Incognito to "browse the web privately." Google emphasizes this again by telling users that they are "in control of what information you share with Google when you search. To browse the web privately, you can use private browsing." Repeatedly, Google mentions that "Chrome," which is a Google-owned product, will not save users' browsing history when they go Incognito. [26]

Google's arguments otherwise do not persuade. First, relying on the Ninth Circuit's decision in *Block v. eBay, Inc.*, Google argues that none of the statements above are enforceable promises. In *Block*, auctioneers argued that eBay had violated two provisions of its User Agreement. 747 F.3d 1135, 1137 (9th Cir. 2014). The Ninth Circuit affirmed the district court's dismissal because the provisions at issue did not include enforceable promises. *Id.* at 1138–39. Specifically, the Ninth Circuit found that statements like "our sites are venues that allow anyone to offer, sell, and buy just about anything," or "[w]e are not involved in the actual transaction between buyers and sellers" were descriptive, not promissory. *Id.* It contrasted these types of statements with ones where the User Agreement said that one of the parties "will" or "will not" do something. *Id.* Those types of statements, the Ninth Circuit said, contained "explicit promissory language." *Id.* Here, Google uses the same type of promissory language. For example, it tells users that Google "won't," save users' browsing information while they are in Incognito mode. Users could read this as creating an enforceable promise. [27]

***13** Second, Google also argues in passing that the alleged promise not to collect users' private browsing data is not supported by consideration. The Court disagrees. Plaintiffs use Google's products, including Incognito mode, and plaintiffs in turn provide Google with vast amounts of information that make it possible for Google, among other things, to sell better advertisements. (PAF 27.) Plaintiffs have evidence to show that this bargained-for exchange covers plaintiffs use of Incognito mode. Moreover, Google does not dispute that the Terms of Service, for example, create an enforceable contract.

Third, Google states that its expert has survey evidence to show most users, including named plaintiffs, understood that Google collects the at-issue data. (SUF 85.) Plaintiffs' expert showed the opposite—he found that, looking at the Incognito Splash Screen, the great majority of users did not expect Google to collect their private browsing history. (Response to SUF 85.) Competing expert opinions raise triable issues barring summary judgment. Moreover, despite Google's argument to the contrary, the named plaintiffs never said that they understood Google was tracking them in Incognito mode. Rather, they testified that, though they understood the Privacy Policy to say that their data is collected when they are

in regular browsing mode, they did not understand the Privacy Policy to say that Google continued to collect their data in private browsing mode. [28]

Finally, Google asks for summary judgment because plaintiffs are only seeking injunctive relief. Not so. Plaintiffs also seek equitable relief, including specific performance which has long been held "a remedy associated with breach of contract." *Pauma Band of Luiseno Mission Indians of Pauma & Yuima Reservation v. California*, 813 F.3d 1155, 1167 (9th Cir. 2015).

For the reasons explained above, the Court **DENIES** Google's motion for summary judgment as to plaintiffs' breach of contract claim.

2. Wiretap Act

With respect to the Wiretap Act claim, Google makes three arguments. First, because the Wiretap Act is a one-party consent statute, and one of the parties, the developers who installed Google's code on their websites, consented to the receipt of the at-issue data, plaintiffs' claim fails. Second, because Google receives the at-issue data in the ordinary course of business, an exception applies. Third, in any event, the data here is not "content" under the Wiretap Act. Plaintiffs dispute each.

a. Developer Consent

The Wiretap Act provides a private right of action against any person who "intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication." 18 U.S.C. § 2511(1)(a); *see also* 18 U.S.C. § 2520 (creating a private right of action for Section 2511). Relevant here, the consent of one party is a complete defense to liability: The statute states that "[i]t shall not be unlawful under this chapter for a person not acting under color of law to intercept a wire, oral, or electronic communication where ... one of the parties to the communication has given prior consent to [the] interception." 18 U.S.C. § 2511(2)(d); *see also Pyankovska v. Abid*, 65 F.4th 1067, 1074 (9th Cir. 2023) (noting that the Wiretap Act is a one-party consent statute). "Moreover, consent is not an all-or-nothing proposition. A party may consent to the interception of only part of a communication or to the interception of only a subset of its communications." *In re Google Location History Litig.*, 428 F.Supp.3d 185, 192 (N.D. Cal. 2019) (cleaned up). Courts apply the reasonable person standard to determine consent. *In re Yahoo Mail Litig.*, 7 F.Supp.3d 1016, 1028 (N.D. Cal. 2014). Again, the burden is on Google to prove consent. *Calhoun*, 526 F. Supp. 3d at 620.

***14** The Court cannot find as a matter of law that website developers consented to Google tracking users' private browsing data. Though the Court takes Google's point that website developers had to consent to Google collecting data *generally* when they added Google' services to their websites, Google has not proven that websites consented to the collection of users' private browsing data in particular. As explained above, *supra*, Section III.A.2 "Express Consent", there is at least a triable issue as to whether the Privacy Policy could be reasonably interpreted to promise that Google would not collect users' data while they were in private browsing mode. Because consent is not an all-or-nothing proposition, website developers could have consented to Google tracking their users while they browsed in regular mode without doing so while users browsed privately.

Google's arguments otherwise do not persuade. To start, nothing in *Rodriguez v. Google LLC*, compels the opposite conclusion. Importantly in that case, plaintiffs conceded that app developers "knowingly agree[d]" to the at-issue data collection but "only insofar as that collection comports with each user's individual privacy expectations." 2021 WL 2026726 at *5 (N.D. Cal. May 21, 2021). This "consent-upon-consent" theory was "plainly untenable" because plaintiffs could not explain how an app developer's consent was somehow predicated on "*every* defensible reading of *every* representation Google makes to *each* of its counterparties." *Id.* Plaintiffs here neither concede that website developers knew about Google's collection of private browsing data (they state the opposite) nor argue that website developer's consent is derivative of users' understanding of the Privacy Policy (they argue developers independently did not consent).

Next, even though one of Google's experts opines that website developers "indisputably" consented to Google's receipt of the at-issue data, the opinion, at best, creates a triable issue. For instance, Google's expert could not affirmatively point to a single website that explicitly consented to Google tracking its users in private browsing mode. All he said was that he "expect[s] that website developers are aware" of how Google collects their users' data, an opinion that is far from conclusive. [29]

For those reasons, the Court finds that a triable issue exists relative to the scope of website developers' consent and the motion for summary judgment is **DENIED.** [30]

b. Ordinary Course of Business Exception

The Wiretap Act provides that a device "being used by a provider of wire or electronic communication service in the ordinary course of its business" is not subject to the Wiretap Act. *Id.* § 2510(5)(a)(i). Though the Ninth Circuit has not yet ruled on the scope of this exception, other courts have found that it provides protection from liability "only where [defendant's] interception *facilitates* the transmission of the communication at issue or *is incidental to* the transmission of such communication." *In re Google Assistant Privacy Litig.*, 457 F. Supp. 3d 797, 818 (N.D. Cal. 2020) (internal citation and quotations omitted). There "must be some nexus between the need to engage in the alleged interception and the provider's ultimate business, that is, the ability to provide the underlying service or good." *Matera v. Google Inc.*, No. 15-cv-4062-LHK, 2016 WL 8200619, at *7 (N.D. Cal. Aug. 12, 2016).

***15** The parties dispute whether the embedded Google services fall within Google's "ordinary course of business." As stated above, the way the interception occurs is not disputed. From this, it is not clear whether the "second GET request" is incidental to the communication between user and website; plaintiffs have evidence that it is an entirely different conversation. *See Facebook Tracking*, 956 F.3d at 608 (holding that those who "surreptitiously duplicate transmissions between two parties," including GET requests like the ones here, are not parties to the communication under the Wiretap Act). Nor does it appear that this second GET request is necessary. Google's own expert acknowledges that developers can disable Google Analytics to "honor visitors' opt-out choices" without crashing the site. (Dkt. No. 907-8, Ex. 80, 6/7/22 Georgios Zervas Rebuttal Report ¶ 46.) That the second GET request is essential for Google's services, like Analytics, to work and is therefore core to Google's advertising business is tangential, at best, to whether it is necessary to "facilitate a transmission of a communication" between a user and a third-party website.

For those reasons, the Court **DENIES** Google's motion for summary judgment on the ordinary course of business exception to the Wiretap Act.

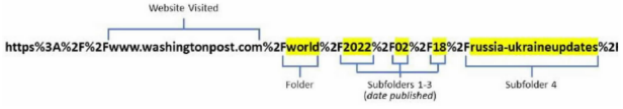
c. Statutory Content

The Wiretap Act applies only to statutorily defined content. Content is defined to "include[ ] any information concerning the substance, purport, or meaning of [the] communication." 18 U.S.C. § 2510(8). In other words, content means "a person's intended message to another." *In re Zynga Privacy Litig.*, 750 F.3d 1098, 1106 (9th Cir. 2014). Not included in the scope of "content" is "record" data like "basic identification and address information." *Id.*

Citing *In re Zynga*, Google argues that plaintiffs' claim fails because the data intercepted here—the GET request—is not "content" but instead "record" information. Plaintiffs disagree, arguing this data contains content—it expresses, for example, the websites visited and pages searched.

In *Zynga Privacy*, plaintiffs sued Facebook and Zynga for disclosing their referer headers to third parties. 750 F.3d at 1103. There, the Ninth Circuit disagreed with plaintiffs that the information contained in a referer header, such as users' Facebook IDs and the web address where the user clicked on a link, fell within the scope of "content" under the Wiretap Act. *Id.* It did so because the Act "refers to the intended message conveyed by the communication, and does not include record information regarding the characteristics of the message that is generated in the course of the communication." *Id.* at 1106. The identification and address information contained in a referer header was not sufficient. *Id.* at 1107. At the same time, the Ninth Circuit noted that, "[u]nder some circumstances, a user's request to a search engine for specific information" could constitute content. *Id.* at 1108–09.

Here, plaintiffs allege that the intercepted communications contain significantly more information, namely the users' IP addresses, referers, user-agents, HTTP requests, users' actions on a website, and their search queries. Though much of this, such as users' IP addresses and their user-agents, is the record, not substance, of the communication, Google collects the type of search queries the Ninth Circuit thought could be content in *Zynga Privacy.* Plaintiffs give the following example:



Once intercepted, Google would know from this communication that the user was searching for updates on Russia's war against Ukraine on the Washington Post's "World" section. This information is not like the "outside of an envelope," revealing the address and name of the recipient, but instead the contents of a letter. *Cf. Zynga Privacy*, 750 F.3d at 1108. In *Facebook Tracking*, the Ninth Circuit held these "full-string detailed URL[s]" are distinct from the IP addresses discussed in *Zynga Privacy*. 956 F.3d at 605. "The URLs, by virtue of including the particular document within a website that a person views, reveal much more information ... divulg[ing] a user's personal interests, queries, and habits." *Id.* at 605. So too here. Google's objection that the example was "generated for litigation" does not negate the dispute created by the evidence showing such information is being collected. ***16** For those reasons, Google's motion for summary judgment as to the Wiretap Act is **DENIED.**

3. California Invasion of Privacy Act (CIPA)

Google seeks judgment on plaintiffs' Section 632 claim on the grounds that the communications at issue are not confidential, namely the GET requests sent by users to third-party websites.[31] Plaintiffs respond that users expect, when using Incognito mode, that those communications will remain private as to Google.

Section 632 provides liability against "[e]very person who, intentionally and without the consent of all parties to a confidential communication, by means of any electronic amplifying or recording device, eavesdrops upon or records the confidential communication." Cal. Penal Code. § 632. CIPA defines a "confidential communication" as:

> any communication carried on in circumstances as may reasonably indicate that any party to the communication desires it to be confined to the parties thereto, but excludes a communication made ... in any [ ] circumstance in which the parties to the communication may reasonably expect that the communication may be overheard or recorded.

Id. at § 632(c). "The standard of confidentiality is an objective one defined in terms of reasonableness." *Faulkner v. ADT Sec. Servs., Inc.*, 706 F.3d 1017, 1019 (9th Cir. 2013) (cleaned up).

When users open Incognito mode, they are met with a Splash Screen. (Incognito Splash Screen.) That page tells users that they can now "browse privately, and other people who use this device won't see your activity." (*Id.*) It warns users, however, that their activity "might still be visible to:" websites they visit, their employer or school, or their internet service provider. (*Id.*) Notably absent from that list is Google itself.

The Court agrees with plaintiffs that a user could reasonably understand the Incognito Splash Screen to disclose that, while users' communications might be accessible (at least in part) to the delineated third parties, they would not be accessible to Google. Indeed, one of the named plaintiffs testified that was his understanding. (PAF 14.)

Google's contrary arguments fail. Google first makes two arguments regarding the meaning conveyed by the Splash Screen. Google says that the Incognito Screen makes clear that privacy in Incognito has limits by telling users that their activity will be visible to *entities online, including* websites, employers, and ISPs. It also argues that, because plaintiffs knew they could be "overheard" by someone else, they had no expectation of privacy against anyone else, including Google. These arguments merely highlight that a material dispute exists over Google's disclosures here. Certainly, they do not persuade as a matter of law. Given the statute defines "confidential communications" as requiring knowledge of the "parties thereto," and plaintiffs have proffered evidence that they did not know that Google was intercepting their communications, there is a reasonable argument that plaintiffs had an expectation of privacy against Google even if they knew others could be listening in. *See* Cal. Penal Code § 632(b) (stating that "parties thereto" mean entities "known by all parties" to be listening in). The Court, again, is guided by the way that Google itself chose to represent its private browsing mode: Google told users that they could "go Incognito" and "browse privately." By browsing privately, plaintiffs could be said to have asserted their expectation of privacy. Google is welcome to make the counterargument at trial.

***17** Second, invoking *Campbell*[32], Google argues that, because websites record users' private browsing activity, users have no expectation of privacy. All electronic communications are recorded; Google argues that means electronic communications are presumptively unprotected by CIPA.

With respect to this argument, the Court begins with the statute. Nothing in Section 632 ties confidentiality to the mode in which a conversation is recorded. Rather, the inquiry is whether "any party to the communication desires it to be confined to the parties thereto." Cal. Pen. Code § 630(c). These is a fact-intensive inquiry. For that reason, CIPA "has been read to require the assent of all parties to a communication before another may listen." *Ribas v. Clark*, 38 Cal.3d 355, 361, 212 Cal.Rptr. 143, 696 P.2d 637 (Cal. 1985); *see also Flanagan v. Flanagan*, 27 Cal.4th 766, 775, 117 Cal.Rptr.2d 574, 41 P.3d 575 (2002) (citing to *Ribas* in support).[33] As stated above, Google has not shown, as a matter of law, that all parties consented to it recording the communications here and therefore summary judgment is not appropriate.

Google's narrower argument, that California courts have developed a presumption that users do not have an expectation of privacy over internet communications, fails on examination. In *Flanagan*, the California Supreme Court resolved a split among its courts of appeal on the standard for confidentiality. It held that confidentiality, under Section 632, requires "nothing more than the existence of a reasonable expectation by one of the parties that no one is listening in or overhearing the conversation." 27 Cal. 4th 766, 773, 117 Cal.Rptr.2d 574, 41 P.3d 575 (Cal. 2002). This was because there is a "critical distinction between eavesdropping upon or recording a conversation and later disseminating its content." *Id.* at 775, 117 Cal.Rptr.2d 574, 41 P.3d 575. By focusing on "simultaneous dissemination, not secondhand repetition" the California Supreme Court held that Section 632 would better fulfill CIPA's legislative purpose of protecting privacy interests. *Id.* In short, Section 632 protects against "intentional, nonconsensual recording" of communications "regardless of the content of the conversation" involved or how parties choose to disseminate it thereafter. *Id.* at 776, 117 Cal.Rptr.2d 574, 41 P.3d 575.

True, the California Supreme Court has not yet opined on the contours of Section 632 confidentiality in the context of internet communications. *See Smith v. LoanMe, Inc.*, 11 Cal.5th 183, 193, 276 Cal.Rptr.3d 746, 483 P.3d 869 (Cal. 2021) (noting that *Flanagan* remains the California Supreme Court's most extensive discussion of the CIPA provisions at issue). Nonetheless, *Flanagan* and its progeny recognized that CIPA was intended to cover newer forms of communication. *See Flanagan*, 27 Cal.4th at 774, 117 Cal.Rptr.2d 574, 41 P.3d 575 (holding that, because Section 632 defines confidential communications as "*includ[ing]*" certain communications, and "includes" is "ordinarily a term of enlargement rather than limitation," Section 632 should be interpreted inclusively); *Smith*, 11 Cal.5th at 191, 276 Cal.Rptr.3d 746, 483 P.3d 869 (noting that the California Legislature has updated CIPA to cover emerging technologies that raise new privacy issues). That said, numerous courts in this district have noted that "California appeals courts have generally found that Internet-based communications are not 'confidential' within the meaning of Section 632, because such communications can easily be shared by, for instance, the recipient(s) of the communications." *Campbell*, 77 F.Supp.3d at 839.[34]

***18** Notwithstanding those findings, California courts have never recognized a legal "presumption" that internet communications are not confidential under Section 632.[35] Those cases refer to *People v. Nakai*, 183 Cal.App.4th 499, 107 Cal.Rptr.3d 402 (2010), which says nothing about a presumption.[36] Instead, the *Nakai* court evaluated the specific circumstances of that case before it. There, the court determined that a criminal defendant did not have a reasonable expectation of privacy over his sexually explicit chats, shared over a Yahoo! Chatroom, with a minor. It did so because: Yahoo!'s Privacy Policy indicated that chat dialogues could be shared to investigate or prevent illegal activity; Yahoo! warned users that chats could be archived; defendant was communicating online with a person he did not know in real life (and who turned out not to be a minor at all); and defendant had expressed during the chats a fear that someone would overhear, suggesting he knew that the communications could be intercepted. 183 Cal.App.4th at 501, 512, 107 Cal.Rptr.3d 402.[37]

Ultimately, *Flanagan* controls and instructs that the question under CIPA is whether, at the time of the conversation, the aggrieved party had a reasonable expectation that it would be "confined to the parties thereto." Cal. Pen. Code § 632(c). On this question, the Court finds a triable issue exists. Given Google's portrayal of Incognito mode and its failure to explicitly notify users it would be among the third parties recording their communications

with other websites, plaintiffs could have had a reasonable expectation of privacy over their private browsing. That these communications occurred over the internet does not automatically mean that plaintiffs gave up that expectation of privacy they had when they went Incognito. Times change, as do modes of communication. What may have been a reasonable expectation in 2006 when *Nakai* was decided is not necessarily so in 2023.

For those reasons, Google's summary judgment motion as to plaintiffs' CIPA claim is **DENIED.**

4. Comprehensive Computer Data and Access Fraud Act (CDAFA)

Google seeks judgment under the CDAFA on the grounds that under the terms of the statute it did not "access" plaintiffs' computers and plaintiffs suffered no "damages or loss." Plaintiffs dispute each.

a. Access

CDAFA creates a private cause of action against any person who "[k]nowingly accesses and without permission takes, copies, or makes use of any data from a computer, computer system, or computer network, or take or copies any supporting documentation, whether existing or residing internal or external to a computer, computer system, or computer network." Cal. Penal Code § 502(c)(2) & (e)(1). Relevant here, "access" means to "cause output from" the "logical, arithmetical, or memory function resources of a computer." *Id.* § 502(b)(1).

Again, the parties do not dispute the way Google receives the at-issue data. (SUF 61.) Here, Google argues it could not have accessed plaintiffs' computers as a matter of law because it is the website developers, not Google, who embed the code which directs users' browsers to send GET requests to Google servers. For this proposition, Google relies on *Meta Platforms, Inc. v. BrandTotal Ltd.*, in which the court found that "reactive data collection" is not within the scope of the CDAFA. 605 F. Supp. 3d 1218, 1260–62 (N.D. Cal. 2022).

***19** *Meta Platforms* is distinguishable. There, an advertising consulting company, BrandTotal, used a browser extension to collect data from Facebook users. *Id.* at 1232. The browser extension worked by collecting information directly from users, not the social media platform itself. *Id.* Meta, Facebook's parent company, sued BrandTotal under the CDAFA and argued that it "accessed" Meta's servers through the browser extension. *Id.* Because the evidence proved otherwise, the court found that BrandTotal was only receiving data directly from users, not the social media platform. *Id.* By contrast here, plaintiffs proffer evidence showing that Google receives data from users' browsers directly, not indirectly through third-party websites. That website developers chose to embed Google's services onto their websites at most creates a triable issue as to whether developers, not Google, "cause output from" plaintiffs' computers. Cal. Penal Code § 502(c)(2).

Google also argues that to hold that it "accesses" plaintiffs' computers in violation of CDAFA would in effect criminalize routine internet functionality and the rule of lenity weighs against such a finding. The Court disagrees. Here, the dispute is about whether Google knowingly accessed plaintiffs' computers "without permission." *See United States v. Christensen*, 828 F.3d 763, 789 (9th Cir. 2015) (citing Cal. Penal Code § 502(c)(2)).[38] If Google can show that it collected the at-issue data with plaintiffs' permission, it would not fall afoul of CDAFA. Given the disputes of fact, a narrower reading of the statute under the rule of lenity is not warranted and summary judgment is not appropriate.

b. Damages or Loss

Second, Google argues plaintiffs suffered no "damage or loss by reason of a [CDAFA] violation." Cal. Pen. Code § 502(e)(1). Plaintiffs disagree and offer evidence showing that they have a stake in the value of their misappropriated data.

Facebook Tracking is instructive. In *Facebook Tracking*, the Ninth Circuit found that plaintiffs had sufficiently alleged their browsing histories carried financial value. *Id.* at 600. So too here. Plaintiffs have evidence that there is a market for their data—Google itself has piloted a program where it pays users $3.00 a day for their browsing history. (PAF 28.) Google responds that *Facebook Tracking* does not apply because it was a decision about standing, not liability. That is beside the point. The Ninth Circuit's decision stands for the proposition that plaintiffs can state an economic injury for their misappropriated data. Because plaintiffs proffer evidence that there is a market for their data—one Google itself has created—the Court cannot rule, as a matter of law, that plaintiffs suffered no damages under CDAFA.

For those reasons, the Court **DENIES** Google's motion for summary judgment as to the CDAFA claim.

5. Invasion of Privacy and Intrusion Upon Seclusion

Google argues both plaintiffs' invasion of privacy and intrusion upon seclusion claims fail because (a) plaintiffs did not have a reasonable expectation of privacy, nor (b) was the intrusion highly offensive. [39] Plaintiffs dispute both.

***20** To state a claim for intrusion upon seclusion in California, a plaintiff must plead that "(1) the defendant intentionally intruded into a place, conversation, or matter as to which the plaintiff has a reasonable expectation of privacy, and (2) the intrusion occurred in a manner highly offensive to a reasonable person." *Facebook Tracking*, 956 F.3d at 601. A claim for invasion of privacy under the California Constitution involves similar elements. *Hernandez v. Hillsides, Inc.*, 47 Cal. 4th 272, 287, 97 Cal.Rptr.3d 274, 211 P.3d 1063 (Cal. 2009); *see also Hammerling v. Google LLC*, 615 F.Supp.3d 1069, 1088 (N.D. Cal. 2022) (so holding).

a. Reasonable Expectation of Privacy

Whether plaintiffs had a reasonable expectation of privacy is an objective inquiry. *Shulman v. Group W Prods., Inc.*, 18 Cal. 4th 200, 231, 74 Cal.Rptr.2d 843, 955 P.2d 469 (1998). "[T]he relevant question here is whether a user would reasonably expect that [Google] would have access to the ... data." *Facebook Tracking*, 956 F.3d at 602. Although Ninth Circuit law indicates that users may not have a reasonable expectation of privacy over the IP addresses of the websites they visit or URLs that only reveal basic identification information, they do over URLs that disclose either unique "search terms" or the "particular document within a website that a person views." *Hammerling*, 615 F.Supp.3d at 1089 (discussing different Ninth Circuit cases).

Facebook Tracking is, again, instructive. There, the Ninth Circuit concluded that users had a reasonable expectation of privacy based on both the nature of the data collection and Facebook's representations to users. 956 F.3d at 602–03. Here, the amount of data collected is indisputably vast—one Google service alone, Analytics, is on over 70 percent of all websites and collects users' data on every visit (Response to SUF 79); the data collected was at least disputably sensitive—as explained, plaintiffs proffer evidence that users go Incognito to search on sensitive topics and so that browsing data may reveal their sexual orientation, political or religious views, or upcoming big purchases; and plaintiffs have put forth evidence to demonstrate that there was a dispute about whether Google has collected this data surreptitiously. As explained above, *see, supra*, Section III.B.2 "Wiretap Act", this information includes much more than just IP addresses or record information. For those reasons, the Court finds that plaintiffs had a reasonable expectation of privacy.

b. Highly Offensive

"Determining whether a defendant's actions were 'highly offensive to a reasonable person' requires a holistic consideration of factors such as the likelihood of serious harm to the victim, the degree and setting of the intrusion, the intruder's motives and objectives, and whether countervailing interests or social norms render the intrusion inoffensive." *Facebook Tracking*, 956 F.3d at 606. "While analysis of a reasonable expectation of privacy primarily focuses on the nature of the intrusion, the highly offensive analysis focuses on the degree to which the intrusion is unacceptable as a matter of public policy." *Id.*

The Court cannot find, as a matter of law, that the data collection here was not highly offensive. Again, plaintiffs have proffered evidence that the data collected here is vast and sensitive. Plaintiffs, further, have put forth evidence that Google's own employees found the data collection problematic. (PAF 12.) Because evidence exists to show that Google did not adequately disclose to users that it was tracking them as they privately browsed, there is at least a triable issue as to whether the intrusion was unacceptable from a public policy perspective.

***21** For those reasons, the Court finds **DENIES** Google's motion for summary judgment as to plaintiffs' invasion of privacy and intrusion upon seclusion claims.

6. Unfair Competition Law (UCL)

Finally, with respect to plaintiffs' UCL claim, Google seeks judgment because: plaintiffs lack standing, and an adequate remedy at law exists, namely money damages. Both lack merit.

Google argues that plaintiffs have not suffered an economic injury because they have not lost money or property. More specifically, with respect to the former, Google notes that plaintiffs did not pay to use any of the at-issue browsers. With respect to the latter, Google contends the data at issue cannot be classified as property because it is not capable of exclusive possession and control. Plaintiffs disagree. They argue their private browsing data has monetary value for which they were not paid and, because the California Consumer Privacy Act affords them the right to exclude Google from selling their data to third parties, they have a property interest in their data.

Under the UCL, a plaintiff must show that they have "suffered injury in fact" and have "lost money or property as a result of their unfair competition." Cal. Bus. & Prof. Code § 17204. The California Supreme Court has held that "there are innumerable ways in which economic injury from unfair competition may be shown." *Kwikset Corp. v. Superior Court*, 51 Cal. 4th 310, 322, 120 Cal.Rptr.3d 741, 246 P.3d 877 (2011). For example, a plaintiff may "surrender in a transaction more, or acquire in a transaction less, than he or she otherwise would have" or "have a present or future property interest diminished." *Id.* at 323, 120 Cal.Rptr.3d 741, 246 P.3d 877.

Sufficient evidence exists that plaintiffs have suffered an injury in fact. Plaintiffs have shown that there is a market for their browsing data and Google's alleged surreptitious collection of the data inhibited plaintiffs' ability to participate in that market. Moreover, plaintiffs have identified an unopposed property interest for at least a portion of the class period under the California Consumer Privacy Act. This applies even if they accessed Incognito mode, for example, for free.

Finally, given the nature of Google's data collection, the Court is satisfied that money damages alone are not an adequate remedy. Injunctive relief is necessary to address Google's ongoing collection of users' private browsing data.

Accordingly, the Court **DENIES** Google's motion for summary judgment as to plaintiffs' UCL claim.

IV. CONCLUSION

For these reasons, the Court **DENIES** Google's motion for summary judgment and **DENIES AS MOOT** plaintiffs' motion to strike. The parties' various motions to seal are **DENIED** to the extent the Court relies on information sought-to-be sealed in this Order but otherwise **CONDITIONALLY GRANTED.**

IT IS SO ORDERED.

All Citations

--- F.Supp.3d ----, 2023 WL 5029899

Footnotes

1 Because the Court denies Google's motion for summary judgment, the Court also **DENIES AS MOOT** plaintiffs' Motion to Strike parts of Google's reply in support of its motion for summary judgment. (Dkt. No. 937.) As to the pending motions to seal, the Court **DENIES** them to the extent it relies on information sought-to-be sealed in this Order. (Dkt. Nos. 907, 924, 933, 936, 939, 942, 945.) For the rest, the Court **CONDITIONALLY GRANTS** them for purposes of this motion. The Court warns parties that it is unlikely that most of the currently-sealed submissions will be kept sealed at trial.

2 For the most part, the parties' arguments are the same regardless of the private browsing mode used, Google's Incognito mode or that of another browser. For that reason, the Court mostly uses these terms interchangeably. Where the type of private browsing mode is material, the Court notes which type of private browsing mode corresponds.

3 Google's Statement of Undisputed Material Facts is referred to here as "SUF"; plaintiffs' Additional Statement of Material Facts is referenced as "PAF." (Dkt. No. 933-3.)

4 The parties also do not dispute that the Google Chrome and Chrome OS Additional Terms of Service are part of the contract. (SUF 15.) Because the parties do not rely upon those two additional writings, the Court does not further address them.

5 Because the Court certified only a Rule 23(b)(2) class (Dkt. No. 803), the Court addresses only the injunctive relief sought on a class-wide basis, not the damages that plaintiffs may later individually seek.

6 These claims arise under the Wiretap Act, CIPA, CDAFA, invasion of privacy, and intrusion upon seclusion.

7 In *Phillips*, the Ninth Circuit held that the "retention of records alone does not constitute a concrete injury." 74 F.4th at ——. The records collected there were from open sources available to the public. *Id.* at ——. Plaintiffs here have evidence of more—they have shown the information collected was private browsing data which Google used to, among other things, sell advertisements. (PAF 27.)

8 PAF 26; Dkt. No. 908-5, Ex. 77, 4/15/22 Expert Report of Jonathan E. Hochman, at 61–62.

9 For example, evidence exists that users go Incognito because what they are searching is sensitive: They want to look up health conditions without being stigmatized, search for ways to exit a relationship without notifying their abuser, shop without being racially profiled, date same-sex partners without being outed. (Dkt. No. 908-5, Ex. 75, 4/15/22 Expert Report of Bruce Schneier, at 25.)

10 In fact, the Ninth Circuit noted that "whether standing could be based entirely on injury from anonymized, aggregated uses of data" remains an open question. *Campbell*, 951 F.3d at 1119 n.9.

11 Dkt. No. 907-7, Ex. 77 ¶ 164 ("Google employees wrote, for example: 'Most users are not aware of session-based tracking. Another internal Google writing notes 'Sign out' is an ambiguous, loaded term that generally means only a portion of what users probably want. Cookies span signed and signed out sessions, so Google and third-party products can connect the dots even if they can't write data to a person's account.' The result is Google logging browsing data on non-Google websites from private-browsing and non-private browsing sessions within the same GAIA logs"); *id.* ¶ 165 ("In addition, Google stores a users' logged-in identifier on non-Google websites ... in its logs .... Whenever a user logs-in on non-Google websites, whether in private browsing mode or non-private browsing mode, the same identifier is associated with the data Google collects from a user's browsing activities on that website. Google further logs all such data (private and non-private) within the same logs and uses these data for serving personalized ads"); *id.* ¶¶ 179, 181 ("Throughout the class period, Google used the private browsing information at issue in this lawsuit to serve users with ads (including targeted ads) in that private browsing session .... Google's internal documents confirm that Google personalized advertisements based on private browsing activities.")

12 In its Order Granting in Part and Denying in Part Class Certification, the Court held that, on Google's affirmative defense of implied consent, individual issues predominated. (Dkt. No. 803.) For that reason, only explicit, not implied, consent is at issue here.

13 The Court finds, again, that "[c]onsent is a defense to plaintiffs' claims" and it is therefore on Google, not plaintiffs, to prove. *See Calhoun, et al. v. Google LLC*, 526 F.Supp.3d 605, 620 (N.D. Cal. 2021); *In re Google RTB*, 606 F.Supp.3d at 949 ("Google bears the burden of proof on consent."). The parties do not identify any Ninth Circuit precedent on whether consent is an affirmative element of or defense to plaintiffs' claims. Google's argument to the contrary is rejected now and for purposes of trial. Notwithstanding the foregoing, the Court reviews all evidence submitted to determine whether a dispute of material fact exists as to express consent.

14 *Calhoun v. Google, LLC*, No. 20-cv-5146-YGR, —— F.Supp.3d ——, 2022 WL 18107184 (N.D. Cal. Dec. 12, 2022). There, this Court found that Google disclosed to users that its data collection is browser agnostic, that

is, that Google told users it was collecting their browsing history regardless of whether they were in Google's Chrome or another browser. *Id.* at ——— – ———, 2022 WL 18107184 at *10–*11.

15 Google repeated at the May 12, 2023, hearing that the Privacy Policy was unambiguous and it was therefore not relying on extrinsic evidence for the proposition that it explicitly disclosed the at-issue data collection.

16 Plaintiffs make two further, and easily disposable, arguments. First, plaintiffs argue that this Court should outright reject many of Google's arguments given Judge Koh's prior rejection at the motions to dismiss stage. As counsel is aware, this Court already rejected this argument in *Calhoun*, ——— F.Supp.3d at ——— n. 8, 2022 WL 18107184, at *12 n.8. It does so for the same reasons here. Second, the attempt to argue the effect of the "sanction orders" on the issue of consent strains credulity. The gamesmanship does not impress. Plaintiffs not only mischaracterize the orders, but they have nothing to do with whether Google can prove explicit consent based on the language of its Privacy Policy. (Dkt. No. 588-1 at 40 ¶ 36 and Dkt. No. 898 at 10.)

17 The parties have included various versions of the Privacy Policy all of which contain substantially the same language except for the sentence about private browsing.

18 Google did not add this sentence to its Privacy Policy until May 2018. (SUF 19.) Because Google is seeking summary judgment on a classwide basis, and plaintiffs allege an ongoing harm that can only be remedied by injunctive relief, the Court considers the latest version of Google's Privacy Policy for this pending motion.

19 Google initially seemed to concede that the post-March-2020 Privacy Policy was incorporated. In moving for summary judgment, Google only asked the Court to consider whether the Incognito Splash Screen and Search & Browse Privately Help Page were incorporated. (SUF 15.) It waited until its reply to ask the Court to find, as a matter of law, that the post-March-2020 Privacy Policy was not incorporated. Though arguments raised for the first time on reply are typically waived, *see Autotel v. Nevada Bell Telephone Co.*, 697 F.3d 846, 852 n.3 (9th Cir. 2012), the Court considers Google's belated argument here.

20 Google's only support for the proposition that the post-March-2020 Privacy Policy is not incorporated is Judge Koh's order on Google's motion to dismiss in *Calhoun*, 526 F.Supp.3d at 621. Initially, Google argued that the Privacy Policy *was* incorporated into the contract. *Id.* Judge Koh decided otherwise. *Id.* That said, in *this case*, Judge Koh found a reasonable user *could* conclude that Google's post-March-2020 Privacy Policy *was* incorporated into the Terms of Service. *Brown II*, 2021 WL 6064009, at *11. While neither finding is binding, Google's waffling only furthers the point that ambiguity exists.

21 The parties provided the Court various versions of the Chrome Privacy Notice. The differences in each are not relevant here.

22 *Rodriguez v. Google LLC*, 2021 WL 6621070, at *4 (N.D. Cal. Aug. 18, 2021).

23 The Privacy Policy only included a line about Incognito mode starting May 2018. Because plaintiffs are seeking only forward-looking relief on a classwide basis, the Court does not consider whether the Incognito Splash Screen was incorporated before then.

24 Google argues that the Search & Browse Privately page is the only one that talks about private browsing generally, and, therefore, the only one that applies to Class 2. Plaintiffs note that the post-2022 Privacy Policy also talks about private browsing through another browser. Further, they assert that Google's representations about Incognito mode are relevant to how users interpret its representations about private browsing generally. The Court agrees that a reasonable user could read the other cited writings as relevant to understanding how Google collects private browsing data generally.

25 In support of its position, Google also points the Court to the Incognito Splash Screens' "Learn More" button, which hyperlinks to an article written by Google called "How Chrome Incognito Keeps Your Browsing Private." (SUF 38.) In that article, Google tells users that Incognito mode does not prevent third-party websites from serving ads to users from Incognito sessions. (SUF 39.) This statement alone does not change the Court's analysis. First, the statement is extrinsic evidence, on which Google cannot rely given its position that the contract is unambiguous. Second, in the Incognito Splash Screen, Google already tells users that their activity might be visible to third-party websites. This statement is consistent. However, it does not tell users that their activity is certainly visible to Google – which is the issue. That there is a triable issue is also supported from a view of the writings as a whole.

26 The Court notes that Judge Koh viewed as debatable Google's repeated attempt to distinguish between what "Chrome" does and what "Google" does. *See* *Brown I*, 525 F.Supp.3d at 1065–66. The Court agrees.

27 Google's reliance on *Hammerling v. Google Inc.*, 2022 WL 17365255, at *11 (N.D. Cal. Dec. 1, 2022) fails for the same reason. In fact, in *Hammerling*, the court distinguished that case from this one because, here, "Google had made *express promises* that it would not save particular data while users were in Incognito mode." *Id.* at *11 n.16.

28 *See, e.g.*, Dkt. No. 908-3, Ex. 49 (Davis Tr.) 102:10–104:1; Dkt. No. 908-4, Ex. 53 (Castillo Tr.) ("It's clear to me that when I'm searching Google in regular mode, and not Incognito mode, that you collect this data"); Dkt. No. 908-2, Ex. 51 (Brown Tr.) 102:12–16 ("So I think anything related to Google in Incognito mode is protected, not collected. I think that's clear by ... the large words that you've gone Incognito [and] ... the invisible spy man on top"); Dkt. No. 908-4, Ex. 54 (Trujillo Tr.) 11–14 ("Well, if I'm in regular mode, then I am aware that information is being collected. If I'm in incognito mode, I am not okay that information is being collected without my consent.")

29 *See* Dkt. No. 907-8, Ex. 80, 6/7/22 Georgios Zervas Expert Rebuttal Report ¶ 49. As an example, this expert cites an example of how news organizations like the New York Times have cracked down on website visitors who were using Incognito mode to get around their paywall. This, Google states, establishes that website developers are "generally aware" Google collects the same data regardless of whether it is from a regular or private mode browser. If anything, this shows the opposite. All the Court can conclude from that example is that news organizations like the New York Times realized that Google was *not* collecting the same data, regardless of mode.

30 Plaintiffs argue that there is at least a triable issue as to whether the crime-tort exception to consent applies. Because the Court finds there was no consent, it declines to reach this argument.

31 Like the Wiretap Act claim, Google argues that plaintiffs' Section 631 claim under CIPA fails because Google did not intercept the "contents" of the communications here. The Court rejects this argument for the same reason. *See* *Brodsky v. Apple, Inc.*, 445 F. Supp. 3d 110, 127 (N.D. Cal. 2020) (holding the analysis for a violation of CIPA and the federal Wiretap Act are the same). The broad types of communication plaintiffs have shown are intercepted here include content. Therefore, defendant's motion for summary judgment on this basis is **DENIED.**

32 *Campbell v. Facebook Inc.*, 77 F.Supp.3d 836, 849 (N.D. Cal. 2014).

33 Google's argument is problematic for another reason—it creates a workaround to CIPA's two-party consent rule. Cal. Penal Code § 630 (holding that an eavesdropper is liable when recording or listening in "without the consent of all parties"). It would mean that if both parties to a communication agree that the communication may be recorded, then another party could simultaneously record the communication also. CIPA requires the opposite.

34 *See also* *In re Google, Inc.*, 2013 WL 5423918, at *22 (N.D. Cal. Sept. 26, 2023) ("Some decisions from the California appellate courts, however, suggest that internet-based communication cannot be confidential."); *Cline v. Reetz-Laiolo*, 329 F. Supp. 3d 1000, 1051 (N.D. Cal. 2018) (There are "numerous cases finding that Internet-based communications are not confidential within the meaning of Section 632, because such communications can easily be shared by, for instance, the recipient(s) of the communications").

35 *Revitch v. New Moosejaw, LLC*, 2019 WL 5485330, at *3 (N.D. Cal. Oct. 23, 2019) ("[I]n California, courts have developed a presumption that Internet communications do not reasonably give rise to [a privacy] expectation."); *Rodriguez*, 2021 WL 2026726 at *6 ("Significantly, the California courts 'have developed a presumption that [i]internet communications do no reasonably give rise to [a confidentiality] expectation ... [for that reason] plaintiffs must plead unique, definite circumstances rebutting California's presumption against online confidentiality.")

36 In any event, the Court agrees with Judge Koh that this case is distinguishable from *Nakai* and the line of district court cases relying on it because, significantly here, in this case "Google's policies did not indicate that data would be collected from users in private browsing mode." *Brown I*, 525 F.Supp.3d at 1074.

37 In *Nakai*, the man convicted of sending sexually explicit messages and pictures to someone he thought was a minor moved unsuccessfully at trial to exclude the online chats as confidential communications under CIPA. *Id.*

38 Google raises a new argument in its reply that, to state a CDAFA claim, plaintiffs must show that Google accessed their computers through technical circumvention. Google's statement that this argument is not new but instead rebuttal is specious. The arguments here have always revolved around contractual consent, not technical circumvention. In any case, Google's argument is belied by *Christensen*, in which the Ninth Circuit articulated different standards between the CDAFA and its federal counterpart and rejected the idea that, under the CDAFA, technical circumvention was necessary. 828 F.3d at 789.

39 Google also repeats the argument that, because the data collected here was anonymized, plaintiffs had no reasonable expectation of privacy. For the reasons stated above, *see, supra*, Section III.A.1 "Standing," the Court rejects this argument.

End of Document